This listing of claims will replace all prior versions, and listing, of claims in the application:

Listing of Claims:

1. (Currently Amended) A method of encryption, of a digital signal processor, comprising:

preprocessing said input message wherein said preprocessing includes a permutation of said input message;

~~(a)~~ partitioning said ~~an~~ input message into matrix elements, wherein said matrix is a square matrix, and diagonally filling said matrix;

~~(b)~~ computing a determinant of said matrix;

~~(c)~~ public key encrypting said determinant; and

~~(d)~~ multiplying said matrix by said encrypted determinant.

2. (Canceled) ~~The method of claim 1, further comprising:~~

~~(a) prior to step (a) of claim 1, preprocessing said input message wherein said preprocessing includes a permutation of the message~~.

3. (Currently Amended) The method of claim 1 ~~2~~, wherein:

~~(a)~~ said permutation ~~of step (a)~~ of claim 1 ~~2~~ is generated by a hash of said input message.

4. (Currently Amended) The method of claim 2, wherein:

~~(a)~~ said permutation ~~of step (a)~~ of claim 1 ~~2~~ is generated by a random sequence.

5. (Currently Amended) The method of claim 1 ~~2~~, wherein:

~~(a)~~ said preprocessing ~~of step (a)~~ of claim 1 comprises ~~2 includes~~ exclusive ORing said message after permutation with generators of said permutation.

6. (Currently Amended) The method of claim 1, wherein:

~~(a)~~ said encrypting ~~of step (c)~~ of claim 1 is public-key encryption.

7. (Currently Amended) The method of claim 6, wherein:

~~(a)~~ said public-key encryption is RSA.

8. (Currently Amended) The method of claim 1, wherein:

~~(a)~~ said partitioning ~~of step (a)~~ of claim 1 first fills the principal diagonal of said matrix.

9. (Currently Amended) A method of encryption for a digital signal processor, comprising:

~~(a)~~ preprocessing said input message wherein said preprocessing includes a permutation of said input message and defining a permutation source;

~~(b)~~ generating a permuted message for an input message employing said permutation source;

~~(c)~~ padding said permuted message with said permutation source to obtain a preprocessed message; and

~~(d)~~ encrypting said preprocessed message with block-based encryption method which has blocks smaller than said preprocessed message.

10. (Currently Amended) The method of claim 9, wherein:

said permutation source is generated by a hash of said input message.

11. (Currently Amended) The method of claim 9, wherein:

said permutation source is generated by a random sequence.

12. (Currently Amended) The method of claim 9, wherein:

said block-based encryption is a public key encryption.

13. (Currently Amended) A method of decrypting, of a digital signal processor, comprising:

~~(a)~~ computing a determinant of a matrix-based encrypted message matrix, wherein said encrypted message was generated by partitioning an input message into matrix elements, wherein said matrix is a square matrix and wherein said matrix encrypted message had preprocessing by a permutation and by applying the inverse of said permutation to the results;

~~(b)~~ private key decrypting of said determinant; and

~~(c)~~ multiplying said matrix by the results of said decrypting ~~step (b).~~

14. (Canceled) ~~The method of claim 13, wherein:~~

~~(a) when said matrix-based encrypted message of step (a) of claim 13 had preprocessing including a permutation, applying the inverse of said permutation to the results of step (c) of claim 13~~.

15. (Previously added) The method of claim 9, wherein said padding includes prepending said permuted message with said permutation source to obtain said preprocessed message.

16. (Previously added) The method of claim 9, wherein said padding includes appending said permuted message with said permutation source to obtain said preprocessed message.